

On the List-Decodability of Random Self-Orthogonal Codes

Lingfei Jin, Chaoping Xing and Xiande Zhang

Abstract—In 2011, Guruswami-Håstad-Kopparty [8] showed that the list-decodability of random linear codes is as good as that of general random codes. In the present paper, we further strengthen the result by showing that the list-decodability of random *Euclidean self-orthogonal* codes is as good as that of general random codes as well, i.e., achieves the classical Gilbert-Varshamov bound. Specifically, we show that, for any fixed finite field \mathbb{F}_q , error fraction $\delta \in (0, 1 - 1/q)$ satisfying $1 - H_q(\delta) \leq \frac{1}{2}$ and small $\epsilon > 0$, with high probability a random Euclidean self-orthogonal code over \mathbb{F}_q of rate $1 - H_q(\delta) - \epsilon$ is $(\delta, O(1/\epsilon))$ -list-decodable. This generalizes the result of linear codes to Euclidean self-orthogonal codes. In addition, we extend the result to list decoding *symplectic dual-containing* codes by showing that the list-decodability of random symplectic dual-containing codes achieves the quantum Gilbert-Varshamov bound as well. This implies that list-decodability of quantum stabilizer codes can achieve the quantum Gilbert-Varshamov bound. The counting argument on self-orthogonal codes is an important ingredient to prove our result.

Index Terms—List decoding, probability method, self-orthogonal codes, random codes.

I. INTRODUCTION

The notion of list decoding was introduced independently by Elias and Wozencraft [4], [5], [18]. Instead of insisting on a unique output of codeword, in the list decoding model the decoder allows to output a list of possible codewords which includes the actual transmitted codeword. Compared with the classical unique decoding model, the model of list decoding allows larger number of corrupted errors. A fundamental problem in coding theory is the trade-off between the information rate and the fraction of errors that can be corrected. For list decoding, we have another important parameter, i.e., the largest list size of the decoder's output. We hope the list size to be small.

From the algorithm point of view, a good list decoding algorithm should have polynomial time, which means that the list size should be at most polynomial in the block length of the code. Researchers have been devoted to finding good list

decodable codes with efficient list-decoding algorithms due to the wide applications to complexity theory and more general for computer science [6], [14], [15], and communications [5]. The fraction of errors δ close to $1 - 1/q$ is more interesting for complexity theory, while it is more attractive for δ close to 0 for communication side. Thus, it is meaningful to consider the full range of possibilities for δ .

A. The Gilbert-Varshamov bound

Before starting our paper, we first introduce the Gilbert-Varshamov bound in coding theory that plays a central role in this paper.

For an integer $q \geq 2$, we define the q -ary entropy function by $H_q(x) = x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x)$. Then it is easy to verify the identity $H_{q^2}(x) = \frac{1}{2}H_q(x) + \frac{1}{2}x \log_q(q+1)$. It has been proved that, with high probability, a random q -ary classical block code (and a random q -ary classical linear block code, respectively) of sufficiently large length with rate R and relative Hamming minimum distance δ satisfies the following q -ary classical Gilbert-Varshamov bound [16]

$$R \geq 1 - H_q(\delta). \quad (\text{I.1})$$

Similarly, with high probability, a random q -ary quantum code of sufficiently large length with rate R and relative symplectic minimum distance δ satisfies the following q -ary quantum Gilbert-Varshamov bound [1]

$$R \geq 1 - H_q(\delta) - \delta \log_q(q+1). \quad (\text{I.2})$$

B. Status of list decoding random codes

It is well known that the list-decodability of classical block codes is upper bounded by the classical Gilbert-Varshamov bound (see [6]), i.e., the tolerance error rate $\delta \leq H_q^{-1}(1-R)$. On the other hand, it was shown in [5] that for a random code with rate $R \leq 1 - H_q(\delta) - 1/L$, it is (δ, L) -list-decodable with probability at least $1 - q^{-\Omega(n)}$. However, it is not obvious to generalize this result to linear codes.

Zyablov-Pinsker [19] established an optimal tradeoff between the rate R and the fraction of errors δ for binary linear codes. The results in [19] can be easily generalized to q -ary codes which shows that the minimum list size of a linear code with rate $1 - H_q(\delta) - \epsilon$ is bounded by $\exp(O_q(1/\epsilon))$. But this bound is exponentially worse than the bound $O(1/\epsilon)$ for arbitrary codes.

In [7], Guruswami-Håstad-Sudan-Zuckerman showed existence of $(\delta, 1/\epsilon)$ -list-decodable linear codes of rate at least $1 - H_2(\delta) - \epsilon$ for binary codes. Although the extension of

L. Jin is with Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China. email: lfjin@fudan.edu.cn.

C. Xing is with Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore. email: xingcp@ntu.edu.sg

X. Zhang is with Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore. She is also with School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui, 230026 China. email: xiandezhang@ntu.edu.sg

The work of C. Xing was supported by the Singapore Ministry of Education under the Tier 1 Grant RG20/13. X. Zhang is partially supported by NSFC under grant 11301503.

the results in [7] to larger alphabets is not easy, Guruswami-Håstad-Kopparty [8] finally managed to show that a list size of $O_q(1/\epsilon)$ suffices to have rate within ϵ of the information-theoretically optimal rate of $1 - H_q(\delta)$. This means that the list-decodability of random linear codes is as good as that of general codes. In the latest development, M. Wootters [17] improved the constant in the list size $O_q(1/\epsilon)$ for random linear codes when the decoding radius δ is close to $1 - 1/q$.

C. Motivation

It is well known that (symplectic) self-orthogonal codes form a useful and important class of linear codes which have found wide applications in communications [9], [12], multiplicative secret sharing [3] and quantum codes [2], etc.. It is natural to ask the question about how well one can list decode a random (symplectic) self-orthogonal code or dual-containing code (a symplectic dual-containing code is a subspace of \mathbb{F}_q^{2n} that contains its dual under the symplectic inner product).

Euclidean self-orthogonal codes are extensively used for construction of linear multiplicative secret sharing [3]. In the event that some dishonest players provide fault shares, we have to carry on error correction to recover the secret. In this scenario, one has to consider decoding of Euclidean self-orthogonal codes.

In quantum coding theory, decoding of a quantum stabilizer code Q obtained from a classical self-orthogonal code C can be reduced to decoding of the symplectic dual code C^{\perp_S} (see Section III.C for details). Therefore, list decoding of dual-containing codes with symplectic inner product plays an important role on quantum decoding.

D. Our work and techniques

In this work, we focus on list decoding of Euclidean self-orthogonal and symplectic dual-containing codes. Surprisingly, our results show that the list-decodability of random Euclidean self-orthogonal codes and symplectic dual-containing codes are as good as that of general random codes and random linear codes, namely, the list-decodability of random Euclidean self-orthogonal codes and symplectic dual-containing codes achieves the classical and quantum Gilbert-Varshamov bounds, respectively. Furthermore, we show that the list decodability of symplectic dual-containing is upper bounded by the quantum Gilbert-Varshamov bound, namely, every symplectic dual-containing code with decoding radius δ and rate bigger than $1 - H_q(\delta) - \delta \log_q(q+1)$ must have exponential list size.

A main technique is the powerful probabilistic fact which says that there is a limited correlation between the linear spaces and Hamming balls. More precisely, it is unlikely that the intersection of a linear subspace spanned by t random vectors from a Hamming ball has size more than $\Omega(t)$. This fact was used in [8] and is also an important ingredient in our proof.

Apart from the above fact, the counting idea on Euclidean (symplectic) self-orthogonal linearly independent vectors and spaces by using solutions of quadratic forms is of great important in computation of probability.

E. Organization

The organization of this paper is as follows. We first review some basic results on self-orthogonal codes and quadratic forms in Subsections II.A and II.B. In Subsection II.3, we briefly discuss construction of random Euclidean self-orthogonal codes based on quadratic forms. Subsection II.D presents list decoding and the Main Theorem I. Subsection II.E is fully devoted to a proof of our Main Theorem I, i.e., Theorem 2.3. In Subsection II.F, we prove a lemma on the number of certain self-orthogonal spaces that is used in the proof of Theorem 2.3. Section III studies list decoding of symplectic dual-containing codes. We present a connection between decoding quantum stabilizer codes and symplectic dual-containing codes in Subsection III.C. Then we show that list decodability of symplectic dual-containing is upper bounded by the quantum Gilbert-Varshamov bound in Subsection III.D. Finally in Subsection III.E we prove our Main Theorem II which says that the list decodability of symplectic dual-containing codes achieves the quantum Gilbert-Varshamov bound.

II. LIST DECODING OF EUCLIDEAN SELF-ORTHOGONAL CODES

A. Euclidean self-orthogonal codes

Let us quickly recall some basic concepts and results in coding theory. As we focus on self-orthogonal codes which are always linear, we assume from now on that q is a prime power and denote by \mathbb{F}_q the finite field of q elements. A q -ary $[n, k]$ -linear code C is a subspace of \mathbb{F}_q^n with dimension k , where n and k are called the length and dimension of the code C , respectively. The information rate of the code C is $R = k/n$ in this case.

Two vectors \mathbf{u} and \mathbf{v} are said Euclidean orthogonal if $\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^n u_i v_i = 0$. A vector \mathbf{u} is said Euclidean self-orthogonal if $\langle \mathbf{u}, \mathbf{u} \rangle = 0$. The Euclidean dual code C^{\perp_E} of a linear code C consists of all vectors in \mathbb{F}_q^n that are orthogonal to every codeword in C . A subset $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ of \mathbb{F}_q^n is called Euclidean self-orthogonal if $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0$ for all $1 \leq i, j \leq t$.

A linear code C is said Euclidean self-orthogonal if $C \subseteq C^{\perp_E}$. It is easy to see that any Euclidean self-orthogonal code has dimension $k \leq \frac{n}{2}$. Hence a self-orthogonal code has information rate $0 \leq R \leq 1/2$.

B. Quadratic forms

An n -variate quadratic form over \mathbb{F}_q is a zero polynomial or homogeneous polynomial of degree 2 in n variables with coefficients in \mathbb{F}_q , i.e.,

$$f(\mathbf{x}) = f(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{F}_q.$$

A fundamental problem in the theory of quadratic form is how much one can simplify $f(\mathbf{x})$ by means of nonsingular linear transformation of indeterminates. Two quadratic forms $f(\mathbf{x})$ and $g(\mathbf{x})$ are said *equivalent* if there exists a nonsingular $n \times n$ matrix A such that the quadratic form $f(\mathbf{x}A)$ is equal to $g(\mathbf{x})$. It is easy to verify that this is indeed an equivalence

relation. Furthermore, two equivalent quadratic forms have the same number of zeros. For a nonzero quadratic form $f(\mathbf{x})$, the smallest number m for which $f(\mathbf{x})$ is not equivalent to a quadratic form in fewer than m indeterminates is called the *rank* of $f(\mathbf{x})$. The rank of the zero quadratic is defined to be 0. If the rank of a nonzero quadratic form $f(\mathbf{x})$ is n , then $f(\mathbf{x})$ is called *non-degenerate*. If \mathbb{F}_q has an odd characteristic, then a quadratic form $f(\mathbf{x})$ can be written as $f(\mathbf{x}) = \mathbf{x}B\mathbf{x}^T$ for a symmetric matrix B of size n over \mathbb{F}_q . The rank of B is in fact equal to the rank of $f(\mathbf{x})$. The reader may refer to [11, pages 278-289] for the details about quadratic forms.

For the purpose of this paper, we are mainly interested in the number of solutions of $f(\mathbf{x}) = 0$ for a quadratic form $f(\mathbf{x})$. We combine several results in [11, Section 6.2] in the following lemma.

Lemma 2.1: Let $f(\mathbf{x}) := f(x_1, \dots, x_n)$ be a quadratic form defined over \mathbb{F}_q with rank m . Denote by $N(f(\mathbf{x}) = 0)$ the number of solutions of $f(\mathbf{x}) = 0$ in \mathbb{F}_q^n . If $m = 0$, then $N(f(\mathbf{x}) = 0) = q^n$. If $1 \leq m \leq n$, then

$$N(f(\mathbf{x}) = 0) = \begin{cases} q^{n-1} & m \text{ is odd;} \\ q^{n-1} \pm (q-1)q^{n-\frac{m}{2}-1} & m \text{ is even.} \end{cases} \quad (\text{II.1})$$

C. Construction of random Euclidean self-orthogonal codes

Unlike construction of a random linear code where one can choose a random set of linearly independent vectors, construction of a random Euclidean self-orthogonal code is not straightforward. In this part, we briefly discuss construction of random Euclidean self-orthogonal codes through quadratic forms.

Note that construction of a random Euclidean self-orthogonal code is equivalent to finding a linearly independent set $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ of random Euclidean self-orthogonal vectors.

We first choose a nonzero random solution $\mathbf{v}_1 = (v_{11}, \dots, v_{1n})$ of the quadratic equation $x_1^2 + \dots + x_n^2 = 0$ (note that this equation has at least q^{n-2} solutions by Lemma 2.1). Then \mathbf{v}_1 is self-orthogonal. Assume that we have already found a linearly independent set $\{\mathbf{v}_1, \dots, \mathbf{v}_{k-1}\}$ of random Euclidean self-orthogonal vectors. If we want to find a k th vector $\mathbf{v}_k = (v_{k1}, \dots, v_{kn})$, then (v_{k1}, \dots, v_{kn}) is a solution of the following equation system

$$\begin{cases} v_{11}x_1 + \dots + v_{1n}x_n = 0, \\ \vdots \\ v_{k-1,1}x_1 + \dots + v_{k-1,n}x_n = 0, \\ x_1^2 + \dots + x_n^2 = 0. \end{cases} \quad (\text{II.2})$$

Substituting the first $k-1$ equations of (II.2) into the last equation of (II.2), we obtain a quadratic equation $g(x_{i_1}, \dots, x_{i_{n-k+1}}) = 0$ of $n-k+1$ variables. Thus, as long as $N(g(x_{i_1}, \dots, x_{i_{n-k+1}}) = 0)$ is bigger than the cardinality of $\text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_{k-1}\}$, i.e., $N(g(x_{i_1}, \dots, x_{i_{n-k+1}}) = 0) > q^{k-1}$, we can randomly choose a solution \mathbf{v}_k of (II.2) which is not contained in $\text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_{k-1}\}$ (note that the number of solution of (II.2) is equal to $N(g(x_{i_1}, \dots, x_{i_{n-k+1}}) = 0)$). Hence, we obtain a linearly independent set $\{\mathbf{v}_1, \dots, \mathbf{v}_{k-1}, \mathbf{v}_k\}$ of random self-orthogonal vectors.

On the other hand, by Lemma 2.1, the number $N(g(x_{i_1}, \dots, x_{i_{n-k+1}}) = 0)$ of solutions of $g(x_{i_1}, \dots, x_{i_{n-k+1}}) = 0$ is at least q^{n-k-1} . Thus, as long as $q^{n-k-1} > q^{k-1}$, i.e., $k \leq (n-1)/2$, we can proceed to the next step to get a basis $\{\mathbf{v}_1, \dots, \mathbf{v}_{k-1}, \mathbf{v}_k\}$.

D. List decoding random Euclidean self-orthogonal codes

First of all, we assume that our channel has adversarial noise. In other words, the channel can arbitrarily corrupt any subset of up to a certain number of symbols of a codeword. Our goal is to correct such errors and recover the original message/codeword efficiently. An error-correcting code C of block length n over a finite alphabet Σ of size q maps a set of messages into codewords in Σ^n . The rate of the code C is defined to be $R := R(C) = \frac{\log_q |C|}{n}$.

The formal definition of list decoding can be stated combinatorially in the following way.

Definition 2.2: For integers $q \geq 2$, $L \geq 1$ and a real $\delta \in (0, 1 - 1/q)$, a q -ary code C of length n over a code alphabet Σ of size q is called (δ, L) -list-decodable if, for every point $\mathbf{x} \in \Sigma^n$, there are at most L codewords whose Hamming distance from \mathbf{x} is at most δn .

Note that while considering (δ, L) -list-decodability, we always restrict the fraction $\delta < 1 - 1/q$ since decoding from a fraction of $1 - 1/q$ or more errors is impossible except for the trivial codes. If we want a polynomial size list, the largest rate R of the code that one can hope is $1 - H_q(\delta)$ [7], [4], [5], [19].

The proof of our main theorem (Theorem 2.3) combines an idea used for random linear codes [8] and the counting result on self-orthogonal linearly independent vectors and spaces by using solutions of quadratic forms.

Theorem 2.3: (Main Theorem I) For every prime power q and a real $\delta \in (0, 1 - 1/q)$ satisfying $1 - H(\delta) \leq 1/2$, there exists a constant M_δ , such that for small $\varepsilon > 0$ and all large enough n , a random self-orthogonal code $C \subseteq \mathbb{F}_q^n$ of rate $R = 1 - H(\delta) - \varepsilon$ is $(\delta, \frac{M_\delta}{\varepsilon})$ -list-decodable with probability $1 - q^{-n}$.

The first step in the proof of Theorem 2.3 is to reduce the problem of the list-decodability of a random Euclidean self-orthogonal code to the problem of studying the weight distribution of certain random linear code containing a given Euclidean self-orthogonal code.

We quote a result from [8] below where $B_n(\mathbf{x}, \delta)$ denotes the Hamming ball with center $\mathbf{x} \in \mathbb{F}_q^n$ and radius δn .

Lemma 2.4: For every $\delta \in (0, 1 - 1/q)$, there is a constant $M > 1$ such that for all n and all $t = o(\sqrt{n})$, if X_1, \dots, X_t are picked independently and uniformly at random from $B_n(\mathbf{0}, \delta)$, then

$$\Pr[|\text{span}(X_1, \dots, X_t) \cap B_n(\mathbf{0}, \delta)| \geq M \cdot t] \leq q^{-(6-o(1))n}.$$

This lemma shows that if we randomly pick t vectors from the Hamming ball $B_n(\mathbf{0}, \delta)$, where t is a constant depending on the list size L , the probability that more than $\Omega(t)$ vectors in the span of these t vectors lies in the ball $B_n(\mathbf{0}, \delta)$ is quite

small. The detail of the proof for this lemma is given in [8]. The key technique for proving this lemma involves a Ramsey-theoretical lemma. Similar result for symplectic distance can be easily reduced to the case of Hamming distance by considering codes with alphabet size q^2 (see Section III).

The second step in our proof uses the following result on the probability that a random linear code of dimension k contains a self-orthogonal subcode of dimension $k-1$ and a given set $\{\mathbf{v}_1, \dots, \mathbf{v}_t\} \subseteq \mathbb{F}_q^n$ of linearly independent vectors. Let \mathcal{C}_k^* denote the set of q -ary $[n, k]$ -linear codes in which every code contains a self-orthogonal subcode of dimension $k-1$.

Lemma 2.5: For any linearly independent vectors $\mathbf{v}_1, \dots, \mathbf{v}_t$ in \mathbb{F}_q^n with $t \leq k < n/2$, the probability that a random code C^* from \mathcal{C}_k^* contains $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ is

$$\begin{aligned} & \Pr_{C^* \in \mathcal{C}_k^*} [\{\mathbf{v}_1, \dots, \mathbf{v}_t\} \subseteq C^*] \\ & \leq \begin{cases} q^{(k+t-n-1)t+2k-1} & \text{if } q \text{ is even;} \\ q^{(k+t-n-2)t+4k-2} & \text{if } q \text{ is odd.} \end{cases} \end{aligned}$$

Hence, we always have

$$\Pr_{C^* \in \mathcal{C}_k^*} [\{\mathbf{v}_1, \dots, \mathbf{v}_t\} \subseteq C^*] \leq q^{(k+t-n-2)t+4k-1}. \quad (\text{II.3})$$

We leave the proof of Lemma 2.5 to the coming Subsection F.

E. Proof of Theorem 2.3

Proof: Pick $M_\delta = 5M$, where M is the constant in Lemma 2.4. Put $L = \lceil M_\delta/\epsilon \rceil$. Finally assume that n is large enough to satisfy (i) $n \geq L$; (ii) the term $o(1)$ in Lemma 2.4 is at most 1; (iii) $n \geq \frac{1}{3(1-R)}(\log_q(2L) + L^2 - L + 3)$, i.e.,

$$q^{-3(1-R)n} \times 2Lq^{L^2-L+3} \leq 1. \quad (\text{II.4})$$

Let C be a random self-orthogonal code with dimension Rn in \mathbb{F}_q^n . To show that C is $(\delta, \frac{M_\delta}{\epsilon})$ -list-decodable with high probability, it is sufficient to show that with low probability that C is not $(\delta, \frac{M_\delta}{\epsilon})$ -list-decodable, i.e.,

$$\Pr_{C \in \mathcal{C}_{Rn}} [\exists \mathbf{x} \in \mathbb{F}_q^n \text{ such that } |B_n(\mathbf{x}, \delta) \cap C| \geq L] < q^{-n}, \quad (\text{II.5})$$

where \mathcal{C}_k denotes the set of q -ary $[n, k]$ -self-orthogonal codes.

Thus, from now on we only need to prove that

$$\Pr_{C \in \mathcal{C}_{Rn}, \mathbf{x} \in \mathbb{F}_q^n} [|B_n(\mathbf{x}, \delta) \cap C| \geq L] < q^{-n} \cdot q^{-(1-R)n}. \quad (\text{II.6})$$

Note that the inequality (II.6) is derived from (II.5) since, for every linear C for which there is a “bad” \mathbf{x} such that $|B_n(\mathbf{x}, \delta) \cap C| \geq L$, there are q^{Rn} such “bad” \mathbf{x} .

Furthermore, the probability at the left side of (II.6) can be transformed into the following.

$$\begin{aligned} & \Pr_{C \in \mathcal{C}_{Rn}, \mathbf{x} \in \mathbb{F}_q^n} [|B_n(\mathbf{x}, \delta) \cap C| \geq L] \\ & = \Pr_{C \in \mathcal{C}_{Rn}, \mathbf{x} \in \mathbb{F}_q^n} [|B_n(\mathbf{0}, \delta) \cap (C + \mathbf{x})| \geq L] \\ & \leq \Pr_{C \in \mathcal{C}_{Rn}, \mathbf{x} \in \mathbb{F}_q^n} [|B_n(\mathbf{0}, \delta) \cap \text{span}\{C, \mathbf{x}\}| \geq L] \\ & \leq \Pr_{C^* \in \mathcal{C}_{Rn+1}^*} [|B_n(\mathbf{0}, \delta) \cap C^*| \geq L], \end{aligned}$$

where C^* is a random $Rn+1$ dimensional subspace containing $\text{span}\{C, \mathbf{x}\}$.

For any integer t with $\log_q L \leq t \leq L$ (and hence $L \leq q^t$), denote by \mathcal{F}_t the set of all tuples $(\mathbf{v}_1, \dots, \mathbf{v}_t) \in B_n(\mathbf{0}, \delta)^t$ such that $\mathbf{v}_1, \dots, \mathbf{v}_t$ are linearly independent and $|\text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_t\} \cap B_n(\mathbf{0}, \delta)| \geq L$. Put $\mathcal{F} = \cup_{t=\lceil \log_q L \rceil}^L \mathcal{F}_t$ and denote by (\mathbf{v}) and $\{\mathbf{v}\}$ the tuple $(\mathbf{v}_1, \dots, \mathbf{v}_t)$ and the set $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$, respectively.

We claim that if $|B_n(\mathbf{0}, \delta) \cap C^*| \geq L$, there must exist $(\mathbf{v}) \in \mathcal{F}$ such that $C^* \supseteq \{\mathbf{v}\}$. Indeed, let $\{\mathbf{u}\}$ be a maximal linearly independent subset of $B_n(\mathbf{0}, \delta) \cap C^*$. If $|\{\mathbf{u}\}| < L$, then we can simply take $\{\mathbf{v}\} = \{\mathbf{u}\}$. Otherwise, we can take $\{\mathbf{v}\}$ to be any subset of $\{\mathbf{u}\}$ of size L . Therefore, we have

$$\Pr_{C^* \in \mathcal{C}_{Rn+1}^*} [|B_n(\mathbf{0}, \delta) \cap C^*| \geq L] \quad (\text{II.7})$$

$$\leq \sum_{(\mathbf{v}) \in \mathcal{F}} \Pr_{C^* \in \mathcal{C}_{Rn+1}^*} [C^* \supseteq \{\mathbf{v}\}] \quad (\text{II.8})$$

$$= \sum_{t=\lceil \log_q L \rceil}^L \sum_{(\mathbf{v}) \in \mathcal{F}_t} \Pr_{C^* \in \mathcal{C}_{Rn+1}^*} [C^* \supseteq \{\mathbf{v}\}] \quad (\text{II.9})$$

$$\leq \sum_{t=\lceil \log_q L \rceil}^L |\mathcal{F}_t| q^{((Rn+1)+t-n-2)t+4(Rn+1)-1} \quad \text{by (II.3)}$$

Thus, to have a good bound on our probability, we need to have a reasonably good upper bound for $|\mathcal{F}_t|$. As in [8], we divide the range of t into two intervals.

(1) If $t < 5/\epsilon$, then

$$\frac{|\mathcal{F}_t|}{|B_n(\mathbf{0}, \delta)|^t} \leq \Pr[|\text{span}(X_1, \dots, X_t) \cap B_n(\mathbf{0}, \delta)| \geq L].$$

Since $L \geq M \cdot t$, by Lemma 2.4 we have

$$|\mathcal{F}_t| \leq |B_n(\mathbf{0}, \delta)|^t \cdot q^{-5n} \leq q^{ntH(\delta)-5n}.$$

(2) If $t \geq 5/\epsilon$, then we have $|\mathcal{F}_t| \leq |B_n(\mathbf{0}, \delta)|^t \leq q^{ntH(\delta)}$ which is just a trivial bound.

Finally, by substituting the value of $R = 1 - H(\delta) - \epsilon$ into the inequality (II.10), we have

$$\begin{aligned} & \Pr_{C^* \in \mathcal{C}_{Rn+1}^*} [|B_n(\mathbf{0}, \delta) \cap C^*| \geq L] \\ & \leq \sum_{t=\lceil \log_q L \rceil}^{\lceil 5/\epsilon \rceil - 1} q^{ntH(\delta)-5n} \cdot q^{(-n+t+Rn-1)t+4Rn+3} \\ & \quad + \sum_{t=\lceil 5/\epsilon \rceil}^L q^{ntH(\delta)} \cdot q^{(-n+t+Rn-1)t+4Rn+3} \\ & = q^{-5n+4Rn} \sum_{t=\lceil \log_q L \rceil}^{\lceil 5/\epsilon \rceil - 1} q^{-\epsilon tn+t^2-t+3} \\ & \quad + q^{4Rn} \sum_{t=\lceil 5/\epsilon \rceil}^L q^{-\epsilon tn+t^2-t+3} \\ & \leq q^{-5n+4Rn} \cdot L \cdot q^{L^2-L+3} + q^{4Rn} \cdot L \cdot q^{-5n+L^2-L+3} \\ & = q^{-n} \cdot q^{-(1-R)n} \times q^{-3(1-R)n} \times 2Lq^{L^2-L+3} \\ & \leq q^{-n} \cdot q^{-(1-R)n} \quad \text{by (II.4).} \end{aligned}$$

This completes the proof. \blacksquare

F. Proof of Lemma 2.5

Let us start with a lemma that will be used in this subsection. Recall that \mathcal{C}_k denotes the set of q -ary $[n, k]$ Euclidean self-orthogonal codes, while \mathcal{C}_k^* denotes the set of q -ary $[n, k]$ -linear codes in which every code contains an Euclidean self-orthogonal subcode of dimension $k-1$.

Lemma 2.6: For any given linearly independent, self-orthogonal set $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ with $t < k < n/2$ in a code $C^* \in \mathcal{C}_k^*$, one can find a self-orthogonal subcode C' of C^* with $\dim(C') = k - 1$ such that C' contains the set $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$.

Proof: Let V be the space spanned by $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$. Let C be a self-orthogonal subcode of C^* of dimension $k - 1$. If V is a subspace of C , then we can simply take $C' = C$. If $t = k - 1$, we can simply take $C' = V$. Now we assume that V is not contained in C and $t < k$. In this case, we must have $\dim(C \cap V) = t - 1 \leq k - 2$. Choose a vector \mathbf{v} from $V \setminus C$. Let $U \subseteq \mathbb{F}_q^n$ be the dual code of $\langle \mathbf{v} \rangle$. Then U has dimension $n - 1$ and the intersection $U \cap C$ has dimension at least $k - 2$. It is clear that $V \cap C$ is contained in $U \cap C$ since $V \subseteq U$. Thus, \mathbf{v} is not contained in $U \cap C$. Furthermore, we can choose a subspace W of $U \cap C$ such that $V \cap C \subseteq W$ and $\dim(W) = k - 2$. Let C' be the space spanned by W and \mathbf{v} . It is clear that W is self-orthogonal since $W \subseteq C$. Moreover, \mathbf{v} is orthogonal to itself and every word in W since $W \subseteq U$. As \mathbf{v} is not contained in W , C' must have dimension $k - 1$. This completes the proof. ■

Case 1: \mathbb{F}_q has even characteristic

If \mathbb{F}_q has even characteristic, then we have the following results from counting arguments.

Lemma 2.7: For $k < n/2$, the cardinality of \mathcal{C}_k^* is at least

$$\frac{(q^{n-k+1} - 1)(q^{n-2k+3} - 1)(q^{n-2k+5} - 1) \dots (q^{n-1} - 1)}{(q^k - 1)(q^{k-1} - 1) \dots (q - 1)}.$$

Proof: Denote by $B_k^{(1)}$ and $B_k^{(2)}$ the cardinalities of \mathcal{C}_k and $\mathcal{C}_k^* \setminus \mathcal{C}_k$, respectively. Then $|\mathcal{C}_k^*| = B_k^{(1)} + B_k^{(2)}$.

Let us consider $B_k^{(1)}$ first. First of all, a vector $\mathbf{x} = (x_1, \dots, x_n)$ is self-orthogonal if and only if $x_1^2 + \dots + x_n^2 = 0$. This quadratic form is equivalent to $x_1^2 = 0$ and hence by Lemma 2.1 it has q^{n-1} solutions.

For a code C_{i-1} in \mathcal{C}_{i-1} , we can span C_{i-1} into a self-orthogonal code C_i in \mathcal{C}_i by adding one self-orthogonal vector in $C_{i-1}^\perp \setminus C_{i-1}$. Hence, we have $q^{n-i} - q^{i-1}$ choices of such a vector. On the other hand, there are $(q^k - q^{k-1})(q^k - q^{k-2}) \dots (q^k - 1)$ choices of k -dimensional basis generating the same code of dimension k . Therefore,

$$B_k^{(1)} \geq \frac{(q^{n-2k+1} - 1)(q^{n-2k+3} - 1) \dots (q^{n-1} - 1)}{(q^k - 1)(q^{k-1} - 1) \dots (q - 1)}.$$

The computation of $B_k^{(2)}$ is a bit different from that of $B_k^{(1)}$ as codes in $\mathcal{C}_k^* \setminus \mathcal{C}_k$ are not self-orthogonal. We first choose a linearly independent, self-orthogonal set of size $k - 1$. One can then span this set into a code in $\mathcal{C}_k^* \setminus \mathcal{C}_k$ by adding a vector in $\mathbb{F}_q^n \setminus C_{k-1}^\perp$. Thus, we obtain a recursive formula and get the following inequality

$$B_k^{(2)} \geq \frac{(q^{n-k+1} - q^{n-2k+1}) \prod_{i=1}^{k-1} (q^{n-2i+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \dots (q - 1)}.$$

The desired result follows from adding $B_k^{(1)}$ with $B_k^{(2)}$. ■

Lemma 2.8: For given t ($t < k < n/2$) linearly independent vectors $\mathbf{v}_1, \dots, \mathbf{v}_t$ in \mathbb{F}_q^n , the number of linear codes $C^* \in \mathcal{C}_k^*$ such that $C^* \supseteq \{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ is at most

$$\frac{(q^{n-2k+3} - 1)(q^{n-2k+5} - 1) \dots (q^{n-2t-1} - 1)(q^n - q^{k-1})}{(q^{k-t-1} - 1)(q^{k-t-2} - 1) \dots (q - 1)}.$$

Proof: Denote by A_k the number of linear codes $C^* \in \mathcal{C}_k^*$ such that $C^* \supseteq \{\mathbf{v}_1, \dots, \mathbf{v}_t\}$. Denote by D a maximal self-orthogonal code in $\text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$. Let $A_k^{(1)}$ denote the number of self-orthogonal codes C^* in \mathcal{C}_k^* such that $\{\mathbf{v}_1, \dots, \mathbf{v}_t\} \subseteq C^*$; and let $A_k^{(2)}$ denote the number of $C^* \in \mathcal{C}_k^*$ such that C^* is not self-orthogonal and $\{\mathbf{v}_1, \dots, \mathbf{v}_t\} \subseteq C^*$.

Case 1: If $\dim(D) = t$, then $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ is a self-orthogonal set. By Lemma 2.6, we can span $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ into a code in \mathcal{C}_k^* .

The counting idea is similar to that in the proof of Lemma 2.7 except for that we first fix t linearly independent vectors $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ and then span them into a larger code. Thus, we have

$$A_k^{(1)} \leq \frac{\prod_{i=t-1}^{k-1} (q^{n-2i+1} - 1)(q^{n-k} - q^{k-1})}{(q^{k-t} - 1)(q^{k-t-1} - 1) \dots (q^2 - 1)(q^k - q^{k-1})}.$$

Similarly, we have

$$A_k^{(2)} \leq \frac{\prod_{i=t-1}^{k-1} (q^{n-2i+1} - 1)(q^n - q^{n-k})}{(q^{k-t-1} - 1)(q^{k-t-2} - 1) \dots (q - 1)}.$$

The desired result follows from adding $A_k^{(1)}$ with $A_k^{(2)}$.

Case 2: If $\dim(D) = t - 1$, then we choose a suitable basis $\mathbf{u}_1, \dots, \mathbf{u}_t$ for $\text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ such that $\mathbf{u}_1, \dots, \mathbf{u}_{t-1} \in D$. In this case, by Lemma 2.6 we can get a code C' of dimension $k - 1$ that contains D , and then a code $C^* := \text{span}\{C', \mathbf{u}_t\}$. Hence,

$$A_k \leq \frac{(q^{n-2k+3} - 1)(q^{n-2k+5} - 1) \dots (q^{n-2t+1} - 1)}{(q^{k-t} - 1)(q^{k-t-1} - 1) \dots (q - 1)}.$$

Case 3: If $\dim(D) \leq t - 2$, then in this case it is impossible to find a code in \mathcal{C}_k^* containing $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$. In other words, $A_k = 0$.

This completes the proof. ■

Case 2: \mathbb{F}_q has odd characteristic

The counting technique for odd q is analogous with that of even q . The only difference here is the number of self-orthogonal vectors.

Note that a vector $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ is self-orthogonal if and only if

$$x_1^2 + \dots + x_n^2 = 0. \quad (\text{II.11})$$

In the case where q is even, the quadratic form (II.11) has rank 1. Hence, by Lemma 2.1 it has q^{n-1} solutions. However, in the case where q is odd, the quadratic form (II.11) has rank n and hence by Lemma 2.1 the number of its solutions is between $q^{n-1} - (q - 1)q^{\frac{n}{2}-1}$ and $q^{n-1} + (q - 1)q^{\frac{n}{2}-1}$. Therefore, the corresponding results of Lemmas 2.7 and 2.8 are slightly different in the case of odd characteristic. We state the results below without proofs.

Lemma 2.9: For $k < n/2$, the cardinality of \mathcal{C}_k^* is at least
$$\frac{(q^{n-k+1} - 1)(q^{n-2k+2} - 1)(q^{n-2k+4} - 1) \cdots (q^{n-2} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

Lemma 2.10: For given t ($t < k < n/2$) linearly independent vectors $\mathbf{v}_1, \dots, \mathbf{v}_t$ over \mathbb{F}_q^n , the number of linear codes $C^* \in \mathcal{C}_k^*$ such that $C^* \supseteq \{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ is at most

$$\frac{\prod_{i=t-1}^{k-1} (2q^{n-2i+1} - 1)(q^n + q^{n-2k+1})}{(q^{k-t-1} - 1)(q^{k-t-2} - 1) \cdots (q - 1)}.$$

Proof of Lemma 2.5: For even q , by Lemmas 2.7 and 2.8, we have

$$\begin{aligned} & \Pr_{C^* \in \mathcal{C}_k^*} [\{\mathbf{v}_1, \dots, \mathbf{v}_t\} \subseteq C^*] \\ &= \frac{|\{C^* \in \mathcal{C}_k^* : C^* \supseteq \{\mathbf{v}_1, \dots, \mathbf{v}_t\}\}|}{|\mathcal{C}_k^*|} \\ &\leq q^{2k-t-1} \left(\frac{q^{k-t+1}}{q^{n-2t+1}} \right)^t \leq q^{(k-n+t-1)t+2k-1}. \end{aligned}$$

For odd q , by Lemmas 2.9 and 2.10, we have

$$\begin{aligned} & \Pr_{C^* \in \mathcal{C}_k^*} [\{\mathbf{v}_1, \dots, \mathbf{v}_t\} \subseteq C^*] \\ &= \frac{|\{C^* \in \mathcal{C}_k^* : C^* \supseteq \{\mathbf{v}_1, \dots, \mathbf{v}_t\}\}|}{|\mathcal{C}_k^*|} \\ &\leq \left(\frac{2q^{n-2k+3} - 1}{q^{n-2k+2} - 1} \right)^{k-t-1} \cdot \left(\frac{q^{k-t} - 1}{q^{n-2t} - 1} \right)^t \\ &\quad \cdot \frac{(q^k - 1)(q^n + q^{n-2k+1})}{q^{n-k+1} - 1} \\ &\leq (3q)^{k-t-1} \left(\frac{q^{k-t}}{q^{n-2t}} \right)^t q^{2k} \\ &\leq q^{(-n+t+k-2)t+4k-2}. \end{aligned}$$

This completes the proof. \square

III. LIST-DECODING OF SYMPLECTIC SELF-ORTHOGONAL CODES

A. Symplectic self-orthogonal codes

To define symplectic inner product, we have to consider a q -ary $[2n, k]$ -linear code C in \mathbb{F}_q^{2n} . Two vectors $(\mathbf{u}_1 | \mathbf{v}_1)$ and $(\mathbf{u}_2 | \mathbf{v}_2)$ are said symplectic orthogonal if $\langle \mathbf{u}_1, \mathbf{v}_2 \rangle - \langle \mathbf{u}_2, \mathbf{v}_1 \rangle = 0$. Note that every vector $(\mathbf{u} | \mathbf{v})$ is symplectic self-orthogonal. The dual code C^{\perp_S} of a linear code C consists of all vectors in \mathbb{F}_q^{2n} that are orthogonal to every codeword in C . A subset $\{(\mathbf{u}_1 | \mathbf{v}_1), \dots, (\mathbf{u}_t | \mathbf{v}_t)\}$ of \mathbb{F}_q^{2n} is called symplectic self-orthogonal if the symplectic inner product of $(\mathbf{u}_i | \mathbf{v}_i)$ and $(\mathbf{u}_j | \mathbf{v}_j)$ are 0 for all $1 \leq i, j \leq t$.

A linear code C is said symplectic self-orthogonal if $C \subseteq C^{\perp_S}$. It is well known that a q -ary $[2n, k]$ -symplectic self-orthogonal code gives a q -ary $[[n, n-k]]$ -quantum code [2]. Thus, we define the rate of C in terms of the associate quantum code, i.e., $R := (n-k)/n$.

Finally, let us define symplectic weight and distance. For a vector $(\mathbf{u} | \mathbf{v}) = (u_1, \dots, u_n | v_1, \dots, v_n) \in \mathbb{F}_q^{2n}$, the symplectic weight is defined to be $\text{wt}_S(\mathbf{u} | \mathbf{v}) = |\{1 \leq i \leq n : (u_i, v_i) \neq (0, 0)\}|$. The symplectic distance of two vectors $(\mathbf{u}_1 | \mathbf{v}_1)$ and $(\mathbf{u}_2 | \mathbf{v}_2)$ is defined to be $\text{wt}_S(\mathbf{u}_1 - \mathbf{u}_2 | \mathbf{v}_1 - \mathbf{v}_2)$.

B. Construction of symplectic self-orthogonal codes

Compared with construction of random Euclidean self-orthogonal codes, construction of random symplectic self-orthogonal codes is much easier. This is because every vector in \mathbb{F}_q^{2n} is self-orthogonal under the symplectic inner product. Again construction of a random symplectic self-orthogonal code is equivalent to finding a linearly independent set $\{(\mathbf{u}_1 | \mathbf{v}_1), \dots, (\mathbf{u}_t | \mathbf{v}_t)\}$ of random symplectic self-orthogonal vectors. We first choose a nonzero random vector $(\mathbf{u}_1 | \mathbf{v}_1) = (u_{11}, \dots, u_{1n} | v_{11}, \dots, v_{1n})$. Assume that we have already found a linearly independent set $\{(\mathbf{u}_1 | \mathbf{v}_1), \dots, (\mathbf{u}_{k-1} | \mathbf{v}_{k-1})\}$ of random symplectic self-orthogonal vectors. If we want to find a k th vector $(\mathbf{u}_k | \mathbf{v}_k) = (u_{k1}, \dots, u_{kn} | v_{k1}, \dots, v_{kn})$, then $(u_{k1}, \dots, u_{kn}, v_{k1}, \dots, v_{kn})$ is a solution of the following equation system

$$\begin{cases} v_{11}x_1 + \cdots + v_{1n}x_n - (u_{11}y_1 + \cdots + u_{1n}y_n) = 0, \\ \vdots \\ v_{k-1,1}x_1 + \cdots + v_{k-1,n}x_n - (u_{k-1,1}y_1 + \cdots + u_{k-1,n}y_n) = 0. \end{cases} \quad (\text{III.1})$$

C. Connection between decoding of quantum stabilizer codes and decoding of symplectic self-orthogonal codes

To simplify our presentation in this subsection, we consider only binary quantum stabilizer codes. Let us briefly describe the background on quantum stabilizer codes and their decoding. The reader may refer to [2], [10], [13] for the details on decoding of quantum stabilizer codes.

The state space of one qubit is actually a 2-dimensional complex space with a basis $\{|0\rangle, |1\rangle\}$. We can simply denote this state space of one qubit by \mathbb{C}^2 . Let $\mathcal{G}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$ be the Pauli group acting on \mathbb{C}^2 , where i is the imaginary unit, I is the 2×2 identity matrix and

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = iXZ.$$

The tensor product $(\mathbb{C}^2)^{\otimes n}$ is called the state space of n qubits. Let \mathcal{G}_n denote the Pauli group acting on $(\mathbb{C}^2)^{\otimes n}$, i.e.,

$$\mathcal{G}_n = \{i^m \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n : m \in \{0, 1, 2, 3\}, \sigma_j \in \{I, X, Y, Z\}\},$$

where the action of an element of \mathcal{G}_n on a state of n qubits is through the componentwise action of σ_i on \mathbb{C}^2 .

Quantum stabilizer codes are defined in the following manner. Let \mathcal{S} be a subgroup of \mathcal{G}_n such that $-I \otimes I \otimes \cdots \otimes I \notin \mathcal{S}$. Then \mathcal{S} is a 2-elementary abelian group. Assume that the 2-rank of \mathcal{S} is k for some $k \in [0, n]$ and \mathcal{S} is generated by $\{g_1, g_2, \dots, g_k\}$. The subgroup \mathcal{S} has a fixed subspace $Q_{\mathcal{S}}$ of $(\mathbb{C}^2)^{\otimes n}$ defined by

$$Q_{\mathcal{S}} = \{\mathbf{v} \in (\mathbb{C}^2)^{\otimes n} : g(\mathbf{v}) = \mathbf{v} \text{ for all } g \in \mathcal{S}\}.$$

The subspace $Q_{\mathcal{S}}$ is called an $[[n, n-k]]$ -quantum stabilizer code and it has dimension 2^{n-k} .

To connect the quantum stabilizer code $Q_{\mathcal{S}}$ with a classical linear code, we define a group epimorphism $\psi : \mathcal{G}_n \rightarrow \mathbb{F}_2^{2n}$ given by

$$\psi(i^m \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n) = (x_1, x_2, \dots, x_n | z_1, z_2, \dots, z_n) = (\mathbf{x} | \mathbf{z}),$$

where x_j, z_j are elements of \mathbb{F}_2 that are determined as below

$$\begin{array}{c|cccc} \sigma_j & I & X & Y & Z \\ \hline x_j & 0 & 1 & 1 & 0 \\ z_j & 0 & 0 & 1 & 1 \end{array}$$

Furthermore, we define a $2n \times 2n$ matrix over \mathbb{F}_2

$$\Lambda = \begin{pmatrix} O & I \\ I & O \end{pmatrix},$$

where O is the $n \times n$ zero matrix and I is the $n \times n$ identity matrix. Then it is easy to see that, for two elements $g, h \in \mathcal{G}_n$, $gh = hg$ if and only if $\psi(g)\Lambda\psi(h)^T = 0$, i.e., $\psi(g)$ and $\psi(h)$ are symplectic self-orthogonal. Through the k generators $\{g_1, g_2, \dots, g_k\}$, we define an $k \times 2n$ matrix over \mathbb{F}_2

$$H = \begin{pmatrix} \psi(g_1) \\ \vdots \\ \psi(g_k) \end{pmatrix}.$$

It is easy to see that H has rank k . Since S is abelian, we have $H\Lambda H^T = \mathbf{0}$. Thus, the binary code C with H as a generator matrix is symplectic self-orthogonal.

Now we briefly review decoding of quantum stabilizer codes. Consider an $[[n, n-k]]$ -quantum stabilizer code Q_S as defined above. Assume that a state of $n-k$ qubits is encoded into a coded state $|\alpha\rangle$ of n qubits. Let $\rho = |\alpha\rangle\langle\alpha|$ be the channel input and let $E\rho E^\dagger$ be the channel output with error $E \in \mathcal{G}_n$, where E^\dagger denotes the Hermitian conjugation of E . By computing the syndrome measurements of the received state, one can determine the binary syndrome \mathbf{s} which is equal to $\psi(E)\Lambda H^T$ (see [10]). To decode, i.e., recover the channel input ρ , it is sufficient to determine the error E . On the other hand, finding E can be reduced to finding $\psi(E)$ (note that the scalar i^m does not affect error). Thus, we turn the problem of decoding quantum stabilizer codes into decoding of C^{\perp_S} (to see this, we notice that H is a parity-check matrix of C^{\perp_S}). Assume that E has at most t errors, i.e., in the representation $E = i^m \sigma_1 \otimes \sigma_2 \otimes \dots \otimes \sigma_n$, there are at most t indices j such that $\sigma_j \neq I$. Thus, the corresponding binary vector $\psi(E)$ has symplectic weight at most t . This implies that we have to find an error $\mathbf{e} = \psi(E) \in \mathbb{F}_2^{2n}$ such that $\text{wt}_S(\mathbf{e}) \leq t$ and $\mathbf{e}\Lambda H^T = \mathbf{s}$. This is exactly the decoding problem of classical codes. To list decode Q_S , we can find the list of all vectors $\mathbf{e} \in \mathbb{F}_2^{2n}$ such that $\text{wt}_S(\mathbf{e}) \leq t$ and $\mathbf{e}\Lambda H^T = \mathbf{s}$. In other words, if \mathbf{x}_0 is a solution of $\mathbf{x}\Lambda H^T = \mathbf{s}$, then we have to find all codewords $\mathbf{c} \in C^{\perp_S}$ such that $\text{wt}_S(\mathbf{c} - \mathbf{x}_0) \leq t$.

D. Upper bound on list decodability of symplectic self-orthogonal codes

Recall that the list decodability of classical block codes is upper bounded by the classical Gilbert-Varshamov bound ([6]). In this subsection, we show a similar result for symplectic self-orthogonal codes, namely, the list decodability of symplectic self-orthogonal codes is upper bounded by the quantum Gilbert-Varshamov bound.

First, we have to give a formal definition of list decoding for a symplectic dual-containing code.

Definition 3.1: For a prime $q \geq 2$, an integer $L \geq 1$ and a real $\delta \in (0, 1/2)$, a q -ary symplectic self-orthogonal code C of length $2n$ over a code alphabet \mathbb{F}_q is called (δ, L) -list-decodable if, for every point $\mathbf{x} \in \mathbb{F}_q^{2n}$, there are at most L codewords in C^{\perp_S} whose symplectic distance from \mathbf{x} is at most δn .

Note that list decoding of C is in fact list decoding of its symplectic dual C^{\perp_S} .

Theorem 3.2: For every prime power q and a real $\delta \in (0, 1/2)$, a q -ary symplectic self-orthogonal code C of length $2n$, decoding radius δ and rate $R > 1 - H_q(\delta) - \delta \log_q(q+1) + o(1)$ must have an exponential list size in n .

Proof: Let k be the dimension of C . Then the rate of C is $R = (n-k)/n$. Pick up a random word $\mathbf{x} \in \mathbb{F}_q^{2n}$ and consider the random variable $X := |B_{2n}^S(\mathbf{x}, \delta) \cap C^{\perp_S}|$, where $B_{2n}^S(\mathbf{x}, \delta)$ is the symplectic ball of radius δn , i.e., $B_{2n}^S(\mathbf{x}, \delta)$ consists of all vectors of \mathbb{F}_q^{2n} that have symplectic distance at most δn from \mathbf{x} . The expected value of X is clearly $|C^{\perp_S}| \cdot |B_{2n}^S(\mathbf{0}, \delta)|/q^{2n}$ which is at least

$$\begin{aligned} & q^{2n-k} \times q^{nt(H_q(\delta) + \delta \log_q(q+1))} \times q^{-2n} \\ &= q^{n(R - (1 - H_q(\delta) - \delta \log_q(q+1)))} = \Omega(\exp(n)). \end{aligned}$$

This completes the proof. \blacksquare

E. List decoding random symplectic self-orthogonal codes

Now we state the list decodability of random symplectic self-orthogonal codes below.

Theorem 3.3: (Main Theorem II) For every prime power q and a real $\delta \in (0, 1/2)$, there exists a constant M_δ , such that for every small $\varepsilon > 0$ and all large enough n , a q -ary random symplectic self-orthogonal code C of length $2n$ and rate $R = 1 - H_q(\delta) - \delta \log_q(q+1) - \varepsilon$ is $(\delta, \frac{M_\delta}{\varepsilon})$ -list-decodable with probability $1 - q^{-n}$.

The proof of Theorem 3.3 is exactly similar to the one of Theorem 2.3 except for the different counting of symplectic self-orthogonal codes. For preparation, we give two lemmas that are needed for the proof of Theorem 3.3.

By considering Hamming ball over alphabet size q^2 , we get a similar result as in Lemma 2.4.

Lemma 3.4: For every $\delta \in (0, 1 - 1/q)$, there is a constant $M > 1$ such that for all n and all $t = o(\sqrt{n})$, if X_1, \dots, X_t are picked independently and uniformly at random from $B_{2n}^S(\mathbf{0}, \delta)$, then

$$\Pr[|\text{span}(X_1, \dots, X_t) \cap B_{2n}^S(\mathbf{0}, \delta)| \geq M \cdot t] \leq q^{-2(6-o(1))n}.$$

Next we prove a result on probability for a symplectic dual-containing code containing a given set $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ of linearly independent vectors in \mathbb{F}_q^{2n} .

Let \mathcal{S}_k denote the set of k -dimensional symplectic self-orthogonal codes in \mathbb{F}_q^{2n} .

Lemma 3.5: For any linearly independent vectors $\mathbf{v}_1, \dots, \mathbf{v}_t$ in \mathbb{F}_q^{2n} , the probability that a random code C from \mathcal{S}_k with C^{\perp_S} containing $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ satisfies

$$\Pr_{C \in \mathcal{S}_k}[\{\mathbf{v}_1, \dots, \mathbf{v}_t\} \subseteq C^{\perp_S}] \leq q^{-kt}. \quad (\text{III.2})$$

Proof: Let us first compute the size of \mathcal{S}_k . Note that every element of \mathbb{F}_q^{2n} is symplectic self-orthogonal. Thus, every k -dimensional self-orthogonal code $C_k \in \mathcal{S}_k$ is spanned from a $k-1$ -dimensional self-orthogonal code $C_{k-1} \in \mathcal{S}_{k-1}$ by adding a vector in $C_{k-1}^\perp \setminus C_{k-1}$. Given the fact that, for two vectors $\mathbf{u}, \mathbf{v} \notin C_{k-1}$, $\langle \mathbf{u}, C_{k-1} \rangle = \langle \mathbf{v}, C_{k-1} \rangle$ if and only if $\mathbf{u} - \lambda \mathbf{v} \in C_{k-1}$ for some nonzero $\lambda \in \mathbb{F}_q$, we know that the number of symplectic self-orthogonal codes C_k containing a fixed symplectic self-orthogonal C_{k-1} is $(q^{2n-2k+2} - 1)/(q - 1)$. On the other hand, every k -dimensional symplectic self-orthogonal code contains exactly $(q^k - 1)/(q - 1)$ symplectic self-orthogonal spaces of dimension $k - 1$. This gives the recursive formula $|\mathcal{S}_k|(q^k - 1)/(q - 1) = |\mathcal{S}_{k-1}|(q^{2n-2k+2} - 1)/(q - 1)$. From this recursive formula, we obtain

$$|\mathcal{S}_k| = \frac{(q^{2n-2k+2} - 1)(q^{2n-2k+4} - 1) \cdots (q^{2n} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}. \quad (\text{III.3})$$

Let V be the linear span of $\mathbf{v}_1, \dots, \mathbf{v}_t$. Then C^{\perp_S} contains $\mathbf{v}_1, \dots, \mathbf{v}_t$ in \mathbb{F}_q^{2n} if and only if C is a subspace of V^{\perp_S} . Thus, the number of symplectic self-orthogonal codes C with C^{\perp_S} containing $\{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ is in fact the number of symplectic self-orthogonal codes in V^{\perp_S} . Since $\dim V^{\perp_S} = 2n - t$, by (III.3) this number is at most

$$\frac{(q^{2n-t-2k+2} - 1)(q^{2n-t-2k+4} - 1) \cdots (q^{2n-t} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}. \quad (\text{III.4})$$

Dividing (III.4) by (III.3) gives the desired result. ■

Proof of Theorem 3.3: Pick $M_\delta = 4M$, where M is the constant in Lemma 3.4. Put $L = \lceil M_\delta/\epsilon \rceil$. Assume that n is sufficiently large.

Let C be a random symplectic self-orthogonal code with rate R , i.e., dimension k of C satisfies $k = (1 - R)n$ in \mathbb{F}_q^{2n} . To show that C^{\perp_S} is $(\delta, \frac{M_\delta}{\epsilon})$ -list-decodable with high probability, it is sufficient to show that with low probability that C^{\perp_S} is not $(\delta, \frac{M_\delta}{\epsilon})$ -list-decodable, i.e.,

$$\Pr_{C \in \mathcal{S}_k} [\exists \mathbf{x} \in \mathbb{F}_q^{2n} \text{ such that } |B_{2n}^S(\mathbf{x}, \delta) \cap C^{\perp_S}| \geq L] < q^{-n}. \quad (\text{III.5})$$

Thus, from now on we only need to prove that

$$\Pr_{C \in \mathcal{S}_k, \mathbf{x} \in \mathbb{F}_q^{2n}} [|B_{2n}^S(\mathbf{x}, \delta) \cap C^{\perp_S}| \geq L] < q^{-n} \cdot q^{k-2n}. \quad (\text{III.6})$$

Furthermore, the probability at the left side of (III.6) can be transformed into the following.

$$\Pr_{C \in \mathcal{S}_k, \mathbf{x} \in \mathbb{F}_q^{2n}} [|B_{2n}^S(\mathbf{x}, \delta) \cap C^{\perp_S}| \geq L] \quad (\text{III.7})$$

$$\leq \Pr_{D \in \mathcal{S}_{k-1}} [|B_{2n}^S(\mathbf{0}, \delta) \cap D^{\perp_S}| \geq L] \quad (\text{III.8})$$

$$= \sum_{t=\lceil \log_q L \rceil}^L \sum_{(\mathbf{v}) \in \mathcal{F}_t} \Pr_{D \in \mathcal{S}_{k-1}} [D^{\perp_S} \supseteq \{\mathbf{v}\}] \quad (\text{III.9})$$

$$\leq \sum_{t=\lceil \log_q L \rceil}^L |\mathcal{F}_t| \cdot q^{-kt}, \quad \text{by (III.2)} \quad (\text{III.10})$$

where D^{\perp_S} is a random $2n - k + 1$ dimensional subspace containing $\text{span}\{C^{\perp_S}, \mathbf{x}\}$ and \mathcal{F}_t is defined in the proof of Theorem 2.3. Note that we use the fact that $\text{span}\{C^{\perp_S}, \mathbf{x}\}$ is symplectic dual-containing whenever C^{\perp_S} is.

(1) If $t < 4/\epsilon$, then

$$\frac{|\mathcal{F}_t|}{|B_{2n}^S(\mathbf{0}, \delta)|^t} \leq \Pr[|\text{span}(X_1, \dots, X_t) \cap B_{2n}^S(\mathbf{0}, \delta)| \geq L].$$

Since $L \geq M \cdot t$, by Lemma 3.4 we have

$$|\mathcal{F}_t| \leq |B_{2n}^S(\mathbf{0}, \delta)|^t \cdot q^{-10n} \leq q^{2ntH_{q^2}(\delta) - 10n} = q^{nt(H_q(\delta) + \delta \log_q(q+1)) - 10n}.$$

(2) If $t \geq 4/\epsilon$, then we have $|\mathcal{F}_t| \leq |B_{2n}^S(\mathbf{0}, \delta)|^t = q^{nt(H_q(\delta) + \delta \log_q(q+1))}$ which is just a trivial bound.

Finally, substituting the value of $k = (1 - R)n$ and $R = 1 - H_q(\delta) - \delta \log_q(q+1) - \epsilon$ into the inequality (III.10), we get

$$\begin{aligned} & \Pr_{C \in \mathcal{S}_k, \mathbf{x} \in \mathbb{F}_q^{2n}} [|B_{2n}^S(\mathbf{x}, \delta) \cap C^{\perp_S}| \geq L] \\ & \leq \sum_{t=\lceil \log_q L \rceil}^{\lceil 4/\epsilon \rceil - 1} q^{nt(H_q(\delta) + \delta \log_q(q+1)) - 10n} \cdot q^{-kt} \\ & \quad + \sum_{t=\lceil 4/\epsilon \rceil}^L q^{nt(H_q(\delta) + \delta \log_q(q+1))} \cdot q^{-kt} \\ & \leq \sum_{t=\lceil \log_q L \rceil}^{\lceil 4/\epsilon \rceil - 1} q^{-\epsilon nt - 10n} + \sum_{t=\lceil 4/\epsilon \rceil}^L q^{-\epsilon nt} \\ & \leq q^{-n} \cdot q^{k-2n}. \end{aligned}$$

This completes the proof.

ACKNOWLEDGMENTS

The authors are grateful to the anonymous referees and Professor Dr. Alexei Ashikhmin for their invaluable and constructive comments and suggestions which have greatly improved the structure and presentation of this paper and make this paper more readable.

REFERENCES

- [1] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.
- [2] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.
- [3] H. Chen, R. Cramer, S. Goldwasser, R. de Haan and V. Vaikuntanathan, "Secure Computation from Random Error Correcting Codes," *Proceedings of 26th Annual IACR EUROCRYPT*, Barcelona, Spain, Springer Verlag LNCS, vol. 4515, pp. 329–346, May 2007.
- [4] P. Elias, "List-decoding for noisy channels," MIT, Res. Lab. Electron., Cambridge, MA, Tech. Rep. 335, 1957.
- [5] P. Elias, "Error-correcting codes for list decoding," *IEEE Trans. Inf. Theory*, vol. 37, no. 1, pp. 5–12, 1991.
- [6] V. Guruswami, "List decoding of error correcting codes," Number 3282 in *Lecture Notes in Computer Science*. Springer, 2004.
- [7] V. Guruswami, J. Håstad, M. Sudan and D. Zuckerman, "Combinatorial bounds for list decoding," *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 1021–1035, 2002.
- [8] V. Guruswami, J. Håstad and S. Kopparty, "On the list-decodability of random linear codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 718–725, 2011.
- [9] A. S. Hedayat, N. J. A. Sloane and J. Stufken, "Orthogonal Arrays: Theory and Applications," Springer-Verlag, NY, 1999.
- [10] K. Y. Kuo and C. C. Lu, "On the Hardnesses of Several Quantum Decoding Problems". CoRR abs/1306.5173 (2013)
- [11] R. Lidl and H. Neiderreiter, *Finite fields*, Cambridge University Press, 1997.
- [12] G. Nebe, E. M. Rains and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, Springer-Verlag, 2006.
- [13] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, 2000.
- [14] M. Sudan, "List decoding: Algorithms and applications," *Theoretical Computer Science*, Exploring New Frontiers of Theoretical Informatics, pages 25–41, 2000.

- [15] S. Vadhan, *Pseudorandomness*, Foundations and Trends in Theoretical Computer Science, 2011.
- [16] R. R. Varshamov, "Estimate of the number of signals in error correcting codes," Dokl. Akad. Nauk, SSSR. 117,739-741,1957.
- [17] M. Wootters, "On the list decodability of random linear codes with large error rates," In the Proceedings of the forty-five annual ACM symposium on Theory of computing, STOC'13.
- [18] J. M. Wozencraft, "List decoding," Quarterly Progress Report MIT, Res. Lab. Electron., Cambridge, MA, vol. 48, 1958.
- [19] V. V. Zyablov and M. S. Pinsker, "List cascade decoding," *Probl. Inf. Transm.*, Vol. 17, no. 4, pp. 29–34, 1981.

Lingfei Jin received her B.A. degree in mathematics from Hefei University of Technology, China in 2009. In 2013, she received her Ph.D. degree from Nanyang Technological University, Singapore. Currently, she is an associate Professor at the School of Computer Science, Fudan University, China. Her research interests include quantum information, cryptography and coding theory.

Chaoping Xing received his Ph.D. degree in 1990 from University of Science and Technology of China. From 1990 to 1993 he was a lecturer and associate professor in the same university. He joined University of Essen, Germany as an Alexander von Humboldt fellow from 1993 to 1995. After this he spent most time in Institute of Information Processing, Austrian Academy of Sciences until 1998. From March of 1998 to November of 2007, he was working in National University of Singapore. Since December of 2007, he has been with Nanyang Technological University and currently is a full Professor. Dr. Xing has been working on the areas of algebraic curves over finite fields, coding theory, cryptography and quasi-Monte Carlo methods, etc.

Xiande Zhang received the Ph.D. degree in mathematics from Zhejiang University, Hangzhou, Zhejiang, P. R. China in 2009. After that, she held postdoctoral positions in Nanyang Technological University and Monash University. Currently, she is a Research Fellow at the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Her research interests include combinatorial design theory, coding theory, cryptography, and their interactions.